Key Developments in the Information Risk Function
A Briefing for Chief Information Officers and Heads of IT Infrastructure

Objective
Once a year, the Information Risk Executive Council provides the Chief Information Officers and Chief Financial Officers at our member companies with an update of the key challenges, developments, and innovations in the Information Risk function. These updates are tailored to provide quick insight into some of the critical strategic management challenges facing Information Risk executives today.

Featured Profiles
Barclays PLC
HSBC Holdings Plc
Teradyne, Inc.
The Allstate Corporation
The Boeing Company
The Progressive Corporation

Intended Audiences
Chief Information Officers
Chief Financial Officers
Heads of Infrastructure
Business Unit General Managers

© 2005 Corporate Executive Board. All Rights Reserved.
Information Risk Executive Council Staff

Managing Director
Mukul Kumar

Practice Manager
Kavitha Venkita

Research Team
Afzalul Bari
Jason Dyett
Mark Higgins
Carsten Schmidt
Michael Scutari
Vikram Siddharth

Executive Director
Glenn Tobin

Creative Solutions Group Staff

Lead Graphic Design Specialist
Ladaska Robinson

Contributing Graphic Design Specialists
Amy Barriale
Rami Bizri
Simaran Kaur
Kimberly Turner

Senior Publications Editor
Debra Berkowitz

Publications Editor
Kevin Mullooly

Note to Members
This project was researched and written to fulfill the research requests of several members of the Corporate Executive Board and as a result may not satisfy the information needs of all member companies. The Corporate Executive Board encourages members who have additional questions about this topic to contact the Board staff for further discussion. Descriptions or viewpoints contained herein regarding organizations profiled in this report do not necessarily reflect the policies or viewpoints of those organizations.

Confidentiality of Findings
This document has been prepared by the Corporate Executive Board for the exclusive use of its members. It contains valuable proprietary information belonging to the Corporate Executive Board, and each member should make it available only to those employees who require such access in order to learn from the material provided herein and who undertake not to disclose it to third parties. In the event that you are unwilling to assume this confidentiality obligation, please return this document and all copies in your possession promptly to the Corporate Executive Board.

Legal Caveat
The Information Risk Executive Council has worked to ensure the accuracy of the information it provides to its members. This report relies upon data obtained from many sources, however, and the Information Risk Executive Council cannot guarantee the accuracy of the information or its analysis in all cases. Further, the Information Risk Executive Council is not engaged in rendering legal, accounting, or other professional services. Its reports should not be construed as professional advice on any particular set of facts or circumstances. Members requiring such services are advised to consult an appropriate professional. Neither the Corporate Executive Board nor its programs is responsible for any claims or losses that may arise from (a) any errors or omissions in their reports, whether caused by the Information Risk Executive Council or its sources, or (b) reliance upon any recommendation made by the Information Risk Executive Council.
Across the past 12 months, members of the Information Risk Executive Council have consistently articulated a profound shift in the way they manage their function. No longer relegated to solely infrastructure or network protection—e.g., firewall management, anti-virus monitoring, etc.—members speak of an emerging charter whose primary challenge is protecting the strategic foundation of the enterprise: its intellectual property and information assets.

Members recognize that while the company can withstand incidents causing operational disruption that may result in revenue loss or impeded performance, attacks on the company’s information assets have profound strategic risk implications. Similarly, with regulatory and privacy mandates showing no signs of abating, the company’s reputational value is increasingly at risk.

From Infrastructure to Information Protection

More than ever, the company’s strategic, financial, and reputational risk profile—and its market value itself—is increasingly reliant on the information risk executive’s ability to effectively manage risks to corporate and customer information.

Council members have proven extremely astute in responding to these emerging strategic and reputational risk areas. Having achieved a satisfactory level of maturity in ensuring infrastructure security, members are now turning their attention toward embedding information protection across the corporate workflow.

The Council is pleased to present best practice excerpts, tools, and benchmarking data to help members work with their cross-functional risk partners to achieve this goal of embedded information protection.

To that end, we are happy to provide further detail and discuss the issues addressed in this summary. We are delighted to continue working with you and your team.

Kavitha Venkita Mukul Kumar Glenn Tobin
Practice Manager Managing Director Executive Director

December 2005
Trend #1: Increasing Scope of Responsibilities: IREC’s 2006 member poll found that most budgets will either remain flat or increase across the next 12 months. This steady growth mirrors the expanded role of information risk across the enterprise. Beginning with the Sarbanes-Oxley Act of 2002, the function has been called on to oversee or collaboratively manage activities outside its traditional, highly technical purview, contributing to the growing portfolio of information risk “services” offered to the business.

A Function in Ascendance

Projected budget increases at member companies...

<table>
<thead>
<tr>
<th>Flat</th>
<th>Increase by less than or equal to 5%</th>
<th>Increase by 10% or more</th>
<th>Decrease by less or equal to 5%</th>
<th>Decrease by 10% or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>35%</td>
<td>16%</td>
<td>38%</td>
<td>5%</td>
<td>6%</td>
</tr>
</tbody>
</table>

...reflect an expanded set of information risk service offerings

<table>
<thead>
<tr>
<th>COMPANY X* Information Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning and Governance</td>
</tr>
<tr>
<td>Policies and Standards</td>
</tr>
<tr>
<td>Data Classification</td>
</tr>
<tr>
<td>Risk Management</td>
</tr>
<tr>
<td>Architecture Design</td>
</tr>
<tr>
<td>Security Training and Awareness</td>
</tr>
<tr>
<td>End-User</td>
</tr>
<tr>
<td>Project Implementation</td>
</tr>
<tr>
<td>Identity Management</td>
</tr>
<tr>
<td>Remote User Security</td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>Vulnerability Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Functional Coordination</td>
</tr>
<tr>
<td>Internal Audit</td>
</tr>
<tr>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>Data Privacy</td>
</tr>
<tr>
<td>Physical Security</td>
</tr>
<tr>
<td>Operational Processes</td>
</tr>
<tr>
<td>Penetration Testing</td>
</tr>
<tr>
<td>Firewall Management</td>
</tr>
<tr>
<td>Patch/Incident Management</td>
</tr>
<tr>
<td>Access Rights Monitoring</td>
</tr>
<tr>
<td>Forensics and Investigation</td>
</tr>
<tr>
<td>Intrusion Detection and Prevention</td>
</tr>
<tr>
<td>Disaster Recovery Testing</td>
</tr>
</tbody>
</table>

Source: IREC Agenda Poll, 2005; IREC research.

© 2005 Corporate Executive Board. All Rights Reserved.
**Trend #2: Improved Operational Effectiveness:** Though the function has grown in size and budget, Information Risk organizations have not abdicated key operational security roles; in fact, leveraging the Council’s Information Risk Competency Diagnostic tool, members self-reported high degrees of success in these kinds of attributes. Leveraging in-house expertise around corporate networks, systems, and audit practices, Council members’ teams excel in traditional technical attributes such as Patch Management and Network Defense and Intrusion Detection.

**Success in “Blocking and Tackling”**

*Members report success in core information security operations such as patch management and network defense*

Performance on Attribute

*Scale of 1 to 5 (1 = Low, 5 = High)*

Two Highest-Performing Attributes

1. Patch Management
2. Network Defense and Intrusion Detection

Average = 2.9

Note: Some attributes removed to improve clarity of illustration.

Full set of attributes are listed on page 28.

© 2005 Corporate Executive Board. All Rights Reserved.
**Trend #3: Relative Shift in Incident Costs:** The 2005 CSI/FBI survey found that estimated losses from security incidents decreased by 61% over 2004. This decrease is partly attributable to success in responding to threats aimed at causing operational disruption. At the same time, however, costs to manage incidents that target sensitive information skyrocketed. Further, while these figures include technical fixes or legal costs, it neglects “soft” costs like loss of competitive advantage or reputational impact.

**Increasing Costs of Information Protection**

*While costs incurred to manage most security incidents have declined over 2004, those associated with unauthorized access and theft have risen significantly*

<table>
<thead>
<tr>
<th>Percentage Change in Cost of Security Incident</th>
<th>2004 Versus 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Access</td>
<td>+21%</td>
</tr>
<tr>
<td>Theft of Proprietary Information</td>
<td>+16%</td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
</tr>
<tr>
<td>System Penetration</td>
<td></td>
</tr>
<tr>
<td>Web Site Defacement</td>
<td></td>
</tr>
<tr>
<td>Laptop Theft</td>
<td></td>
</tr>
<tr>
<td>Misuse of Public Web Application</td>
<td></td>
</tr>
<tr>
<td>Insider Net Abuse</td>
<td></td>
</tr>
<tr>
<td>Telecom Fraud</td>
<td></td>
</tr>
<tr>
<td>Financial Fraud</td>
<td></td>
</tr>
<tr>
<td>Abuse of Wireless Networks</td>
<td></td>
</tr>
<tr>
<td>Denial of Service</td>
<td></td>
</tr>
</tbody>
</table>

Source: 2005 CSI/FBI Survey; IREC research.
Trend #4: Change in Enterprise Risk Profile: The dramatic rise in “unauthorized access” and “theft of proprietary information” costs are particularly disconcerting because the assets at greatest risk from these attacks are, in essence, the lifeblood of the corporation—its intellectual property. While a denial of service attack may incur costly downtime, companies understand that attacks targeting intellectual property have a far greater impact to the corporation’s strategic goals and fiscal solvency. Internal Auditors are taking note; key audit “hot spots” across the next 12 months focus on IT risks and business activities reliant on information systems.

“Crown Jewels” Increasingly at Risk

Inability to protect information directly imperils the corporation’s market value…

...contributing to heightened internal audit scrutiny around technology and IT-related business risks

Primary Inflector of the Corporation’s Market Value

Illustrative

Top 2006 Audit “Hot Spot” Dashboard

Illustrative

<table>
<thead>
<tr>
<th>Rank</th>
<th>Hot Spot</th>
<th>Change Versus 2005</th>
<th>Related Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Technology</td>
<td>+4</td>
<td>Reputational, Compliance, and Authentication</td>
</tr>
<tr>
<td>2</td>
<td>Emerging Markets</td>
<td>+8</td>
<td>Political, Economic, and Legal</td>
</tr>
<tr>
<td>3</td>
<td>Business Process Outsourcing</td>
<td>+6</td>
<td>Business Disruption, Confidentiality Violations, Technology Integration</td>
</tr>
<tr>
<td>4</td>
<td>Mergers and Acquisitions</td>
<td>New</td>
<td>Post-Acquisition Integration</td>
</tr>
<tr>
<td>5</td>
<td>Corporate Reputation</td>
<td>New</td>
<td>Lawsuits, Corporate Malfeasance</td>
</tr>
</tbody>
</table>

Source: Pricewaterhouse Coopers Survey; Audit Director Roundtable research; IREC research.
Trend #5: Volatile Regulatory Landscape: Members also face a complex compliance landscape where the corporation’s reputational profile is at risk and the non-legal costs of compliance activities often exceed actual legal costs. With regulatory demands showing no signs of abating, information risk executives must not only recalibrate existing processes to drive cost-effective compliance but also ensure that other, equally critical risk management activities receive the necessary amount of resources.

More Than Sarbanes-Oxley

Perennial and potentially expanding regulatory demands…

Existing and Proposed Privacy-Related Legislation in U.S.

Partial Listing

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>FCRA</td>
<td></td>
</tr>
<tr>
<td>COPPA</td>
<td>CA 1386</td>
<td></td>
</tr>
<tr>
<td>35+ Proposed Bills</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer Privacy Protection Act (H.R.1263)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID Theft Notification Bill (S.1408.IS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPY ACT (H.R. 2929)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPYBLOCK (S.2145)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

…whose impact on the information risk function is significant…

Compliance-Related Implications for the Information Risk Officer

<table>
<thead>
<tr>
<th>Strategic</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Policy redesign</td>
<td>• Systems and documentation costs</td>
</tr>
<tr>
<td>• Regulatory overlap identification and rationalization</td>
<td>• Costs of non-compliance</td>
</tr>
</tbody>
</table>

Operational

<table>
<thead>
<tr>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compliance versus business flexibility</td>
</tr>
<tr>
<td>• Impact to technical environment</td>
</tr>
<tr>
<td>• Identity management implementation</td>
</tr>
<tr>
<td>• Compliance tracking</td>
</tr>
</tbody>
</table>

…threaten to supersede other critical risk management activities

Paved with Good Intentions

“Just because we check off boxes doesn’t mean we’re more secure. In fact, though many of the regulations mean well, I’m concerned we’ll end up selling short other more important risk management activities. I want compliance to be an embedded part of how we do business, not a distraction from more pressing matters.”

CISO
Fortune 500 Electronics Manufacturer

Source: IREC research.
Information Risk Organization’s Mandate: With costs to manage attacks on intellectual property rising, members are playing a heightened role in protecting the critical inflectors of the corporation’s market value. Simultaneously, compliance mandates continue to increase in scope, solidifying members’ role to help manage risks that can adversely affect the company’s reputation. As a result of this confluence of demands, the information risk officer’s charter has transcended traditional “firewall protection” to include the management of risks that can impact the corporation’s market value.

Information Risk as the Steward of the Corporate Brand

At the intersection of strategic business and regulatory risks, the information risk officer is positioned to leverage technical expertise to help reduce the enterprise risk profile

CEO’s Enterprise Risk Dashboard

Illustrative

<table>
<thead>
<tr>
<th>Strategic Risks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Confidential Information</td>
<td>Y</td>
</tr>
<tr>
<td>Geopolitical Unrest in Emerging Markets</td>
<td>Y</td>
</tr>
<tr>
<td>Ineffective M&amp;A Integration</td>
<td>G</td>
</tr>
<tr>
<td>Failure to Identify Emerging Markets/Competitor Actions</td>
<td>Y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regulatory Risks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Compliance with Regulations</td>
<td>G</td>
</tr>
<tr>
<td>Financial Reporting Errors</td>
<td>G</td>
</tr>
<tr>
<td>Significant Overinvestment in Compliance Activities</td>
<td>Y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial Risks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unforeseen Shift in Market Dynamics</td>
<td>R</td>
</tr>
<tr>
<td>Margin Erosion</td>
<td>Y</td>
</tr>
</tbody>
</table>

Areas of Information Risk Overlap

CISO plays a critical role in owning or collaboratively managing key enterprise risks with strategic, regulatory, and reputational impact.

Source: CFO Executive Board research; IREC research.
From Infrastructure to Information Protection: Given the fluidity of the corporate IT environment, the expansion of the extended enterprise, and the proliferation of wireless devices, companies need to do more than secure infrastructure to prevent costly security incidents. Council members have taken note, as their 2006 priorities point to the other half of this critical equation: partnering with business users to collaboratively protect information assets. Therefore, with policies and risk assessments serving a foundation, members are tackling a new set of activities requiring a more proactive, end-user-attuned approach to information risk management.

### Foundational Capabilities for Information Risk Management

#### The Information Risk Management Stack

**Schematic**

| Performance Measurement and Communication |  |
| End-User Awareness and Education |  |
| Regulatory Compliance Enablement |  |
| Operational Process Execution |  |
| Security Architecture Design and Implementation |  |
| Risk Assessment and Mitigation |  |
| Policy Development and Enforcement |  |

**Critical Success Factors**

- Ability to articulate business implications of information risk performances
- Segment-specific message delivery
- Strong cross-functional collaboration
- Process-driven, “always on” controls
- Business-focused response prioritization
- Standardized process execution
- Flexible architecture that compliments procedural/nontechnical controls
- Common “risk vocabulary” for transparent risk management
- Pragmatic (implementable) policies
- Enterprise-wide buy-in

**Case Example**

- **Barclays**
- **HSBC**
- **Allstate**
- **Boeing**
- **Progressive**
- **Regency plc**
- **Prospero Bank**

* Pseudonym.

Source: IREC research.
Policy Development and Enforcement: While many organizations acknowledge the importance of “business-focused” policies, in practice, results are often riddled with technical references that leave end users disengaged. Further, policies fail to educate end users as to how their behavior imperils the enterprise. Upon aggregating key risk inputs and business partner feedback, best-in-class policies can raise awareness, help quantifiably track risks to business strategy, and serve as a “single source of truth” for business negotiations.

Moving Beyond Tech-Speak

Key Attributes of an Effective Information Risk Policy

Excerpt from Company X

Electronic Information Management and Retention Policy
To: All ‘X’ Company Employees and all consultants, contractors and vendors working for ‘X’ Company
Date: June 2005
Subject: Electronic Information Management and Retention Policy

Overview
All records are owned by ‘X’ Company as a corporate asset or intellectual property. To ensure accountability throughout their lifecycle, these records are assigned to a business or functional group for their management.

Applies To
• All ‘X’ Company employees and all consultants, contractors, and vendors working for ‘X’ Company.
• All of ‘X’ Company including all businesses, functional areas, roles, and responsibilities within the organization, joint ventures, and all regions and locations.
• All central and local electronic business systems and collaborative/desktop tools containing information relating to ‘X’ Company.
• All record types and all media used in active or inactive electronic storage.

Objectives
• Ensure adequate records to meet all business and regulatory requirements
• Ensure assigned accountability for all electronic records with an assigned disposition
• Ensure properly categorized records at all stages of the information lifecycle

Policy
• Anyone who creates or receives, either directly or indirectly, any electronic record must categorize the information according to classifications that include retention and accountability rules.
• The accountable party is responsible for reviewing these records and ensuring their appropriate disposition and retention.
• Using the appropriate storage systems, such accountable parties, must ensure the protection and preservation of these records for their full lifecycle.
• All records not required for business or regulatory purposes must be destroyed.

Compliance
• Compliance with this policy will be audited and reported. Individuals will be held responsible for policy violations. Breaches of these policies are also in direct conflict and violation of the ‘X’ Company Code of Business Conduct and can result in termination of employment and/or legal action.

Source: IREC research.
Policy Development and Enforcement: In an effort to build risk mitigation controls early into the new application lifecycle, Allstate’s business impact index provides clear guidelines to application developers on implementing information protection decision rules. By linking the business impact of a new project to the level of required authentication controls, Allstate ensures that its data security policies are front-loaded into the application development lifecycle.

**Calibrated Security Requirements**

*Allstate’s business impact index quantifies risk…*

**Business Impact Index**

<table>
<thead>
<tr>
<th>Project Name:</th>
<th>Life Insurance Sales Application</th>
<th>Sponsor:</th>
<th>John Miller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Classification (DC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential</td>
<td>✓</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Restricted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Criticality (BC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low—Systems that don’t serve customer support or are revenue generating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium—Systems that support business transactions not critical to daily operations</td>
<td>✓</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>High—Systems that support business transactions critical to conduct business or support customer service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accessibility (A)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inside—Components located completely inside Allstate network</td>
<td>✓</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Outside—Outside the boundaries of Allstate’s networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Index (2 x DC + BC + A)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...and, through design requirements, guides principled risk mitigation

**Business Impact Authentication Requirement**

<table>
<thead>
<tr>
<th>Business Impact</th>
<th>Authentication Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 to 5</td>
<td>Identification</td>
</tr>
<tr>
<td>6 to 7</td>
<td>Login and password with expiration</td>
</tr>
<tr>
<td>8 to 9</td>
<td>Digital certificate</td>
</tr>
<tr>
<td>10 to 11</td>
<td>Authentication at both ends</td>
</tr>
<tr>
<td>12 to 13</td>
<td>Two factor with token or biometric</td>
</tr>
</tbody>
</table>

Source: The Allstate Corporation; IREC research.
**Policy Development and Enforcement:** In an effort to mitigate risk across the enterprise, Teradyne drives policy transparency through business risk acceptance and dispute-resolution processes. Leveraging business risk acceptance reports, the CISO approves, waives, or rejects accepted business risks based on their compliance with policies. Should the business push back on rejected risks, policies are weighed against revenue-focused negotiation criteria to drive solutions that mitigate risk while enabling business flexibility.

---

**Managing “Unacceptable” Risks**

*Teradyne’s formalized dispute-resolution process narrows the scope of “unacceptable” risks and drives business-focused resolution*

---

**Teradyne’s Formalized Dispute-Resolution Process**

<table>
<thead>
<tr>
<th>Communication of Critical Risk</th>
<th>Accepted Risk Collection</th>
<th>Up-Front Risk Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>35%</td>
<td></td>
</tr>
</tbody>
</table>

Unresolved risks are prioritized and sent to business units to mitigate or accept. Accepted risks are forwarded to CISO. CISO approves, waives, or rejects accepted risks according to security policy.

**Principal Negotiation Criteria**

- **Business Value at Risk:** What is the impact of a breach on the enterprise as a whole? Can a cheaper fix mitigate risk to an acceptable level?
- **Risk Versus Revenue Potential:** Does the required fix restrict existing or future business activities?
- **Regulatory Impact:** Does the risk have regulatory implications?

**Consensus-Driven Risk Negotiation**

“Unacceptable” risks discussed by leveraging key negotiation criteria.

**Risk Escalation**

Unresolved risks escalated to IT Security Steering Committee.

**Negotiated Approval/Waiver**

Participants reach consensus around preserving business goals while reducing risk.

**Business Spending Alignment**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>$$$</td>
</tr>
<tr>
<td>M</td>
<td>$</td>
</tr>
<tr>
<td>L</td>
<td>$</td>
</tr>
</tbody>
</table>

Negotiations surface risk areas where business is overinvesting.

---

*Source: Teradyne, Inc.; IREC research.*
Risk Assessment and Mitigation: Risk assessments are a core component of the information risk executive’s management portfolio, yet many companies consistently cite low rates of business user adoption of recommendations. This lack of buy-in suggests an inability to create meaningful recommendations aligned to the business’s unique risk profile. By leveraging a more business-focused approach to risk assessments, organizations can promote adoption of recommendations, enable informed trade-off negotiations with key stakeholders, and build a “common vocabulary” to collaborative manage risk.

Five Principles of an Effective Risk Assessment

Recognizing that technology alone cannot effectively capture information risks, exemplars engage partners across assessment activities to ensure accurate, meaningful, and actionable findings

1. Leverage Compliance Urgency to Drive Assessment Participation
   Partner with Internal Audit to communicate the importance of active business participation in assessment activities such as asset valuation and mitigation negotiations.

2. Narrow the Subjectivity of Asset Valuations
   Rather than arbitrarily scoring assets on a multi-point scale, objectively scope business value at risk by asking “yes or no” questions such as “Could the business withstand this risk if it were reported only once?” or “Could the business withstand this risk if it were picked up by the media?”

3. Qualitatively Gauge Business Risk Tolerance
   As automated tools often fail to capture the nuances of the business’s risk tolerance, determine how much financial and nonfinancial loss partners can withstand to help create meaningful recommendations.

4. Transcend Technical Controls When Determining Residual Risk
   A dynamic threat environment that targets the individual rather than the system requires Information Risk to surface business-articulated security and process deficiencies to attain more comprehensive view of residual risk.

5. Facilitate Tolerance-Informed Trade-Off Negotiations
   Leverage articulated tolerance levels to drive mitigation negotiations and subsequent recommendations that address the partner’s unique risk appetite.

Source: IREC research.
Risk Assessment and Mitigation: Acknowledging that seemingly minor risks can adversely affect the enterprise as a whole, Regency plc,* a UK-based financial services firm, standardizes its scoring and reporting tools to normalize diverse IT risks and drive functional prioritization and gap analysis. By deploying a standardized toolset across all corporate functions, Regency stakeholders also leverage aggregated, “apples-to-apples” analyses of IT and non-IT risks, facilitating informed decision making at the enterprise level.

**IT Risk in an Enterprise Context**

*Corporate risk integrates prioritized IT outputs with cross-functional interdependent risk*

---

**Enterprise Key Risk Report**

**Enterprise-Level Risk Tolerance Bands**
- High—Risks that warrant immediate executive attention
- Moderate—Risks addressed at the executive level
- Low—Risks comparatively deprioritized

**Report Key**
- Gross risks
- Net risks
- Movement since last report

---

**Risk Key**

- High-impact/low-likelihood risks are deemed “Moderate/High.”
- High-likelihood/low-impact risks are rated “High.”

---

**Risk Assessment and Mitigation:**

<table>
<thead>
<tr>
<th>Risk Number</th>
<th>Risk Class/Category</th>
<th>Specific Risk Description</th>
<th>Business Owner</th>
<th>Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operational/Systems</td>
<td>1.1 Business A: Inadequate IT infrastructure leads to significant customer service downtime</td>
<td>XXX</td>
<td>G</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2 Business B: IT platform inadequate to meet grown and product ambition</td>
<td>XXX</td>
<td>G</td>
</tr>
<tr>
<td>2</td>
<td>Regulatory Compliance/Data</td>
<td>2.1 Business D: Inadequate access monitoring around application</td>
<td>XXX</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>Regulatory Compliance</td>
<td>3.0 Business A: Further legislative action affecting the financial services industry</td>
<td>XXX</td>
<td>G</td>
</tr>
<tr>
<td>4</td>
<td>Strategic</td>
<td>4.0 Business E: Potential executive staff turnover</td>
<td>XXX</td>
<td>G</td>
</tr>
</tbody>
</table>

* Pseudonym.

Source: Regency plc; IREC research.
Risk Assessment and Mitigation: Lacking codified authority of business users, IT risk analysts at Prospero Bank,* a European-based financial services firm, hold Application Risk Workshops, which gather key end users, IT staff, and executive sponsors to identify risks to business assets and negotiate mitigation trade-offs based on the business’s unique risk appetite. By aligning risk assessment findings to users’ risk tolerance levels—rather than applying a “once size fits all” controls framework—Information Risk helps drive the voluntary adoption of security recommendations.

A Road Map for Business Risk Mitigation

Prospero ensures that application risk assessments are predicated on the business’s articulation of risk impact and tolerance levels

Prospero Application Risk Workshop

Schematic

1 Business Impact Brainstorming
Participants identify the impact of risks to key information

<table>
<thead>
<tr>
<th>Key Information</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prospect Database</td>
<td>Unauthorized external access to sensitive information</td>
</tr>
</tbody>
</table>

Project: CRM Upgrade

2 Scenario Impact Assessment
Participants identify and rate severity of risk impact scenarios

<table>
<thead>
<tr>
<th>Business Severity Rating</th>
<th>Threat Likelihood Forecasting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Survival Threatened</td>
<td>3</td>
</tr>
</tbody>
</table>

3 Threat Likelihood Forecasting
Participants identify threats, mitigating controls, and likelihood for high-impact risks

<table>
<thead>
<tr>
<th>Threat</th>
<th>Current Mitigating Factors</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering Attack</td>
<td>+ Strong provisioning – No awareness campaigns for contractors</td>
<td>Highly Possible</td>
</tr>
</tbody>
</table>

4 Mitigation Trade-Offs
Participants consider multiple mitigation strategies according to business risk tolerance

Control Requirements
- Intern and consultant awareness campaigns
- Quarterly revisits of access rights controls

Source: Prospero Bank; IREC research.

* Pseudonym.
Security Architecture Design and Implementation: Faced with critical and time-sensitive information risk management activities such as identity management, regulatory compliance, and data classification, organizations often deploy projects in an ad hoc and uncoordinated manner. By failing to consider unique business demands, policy implications, and end-user behavior, security initiatives often require costly post-implementation redesign and yield diminished business benefits.

**Holistic Strategy for Information Protection**

*Companies’ disjointed, technically-focused approach to information protection often fails to consider key business and governance factors critical for success*

Technology-Focused Information Protection

- Device protection does not include mobile device.
- User directory does not allow for faster-turnaround access-rights monitoring.
- DRM is protection not linked to user access-right system.
- Two-factor authentication solution does not include integration of external users.

Integrated Information Protection

- Policy
- Process
- Technology
- Behavior

Source: IREC research.
Security Architecture Design and Implementation: Addressing unchecked access rights that increase the risk of costly business outages, Progressive rolls out a formal role redefinition and rationalization initiative. Leveraging inputs from HR, end users, and managers, Progressive redefines role definition and access mapping activities to produce a principled and manageable set of users who can access systems. Progressive’s efforts dramatically reduce profile complexity, the number of roles, and saves the company $1.5 million in reduced downtime.

(Re)Defining Access Rights

A structured approach to role definition reduces risk and complexity in managing access

1. Targeted Interviewee Selection
   HR provides inputs to balance the need for detailed user knowledge with interview volume constraints

2. Holistic View of Permissions
   Information Security consolidates current access permissions

3. Pre-Interview Access Review
   Information Security identifies suspect permissions before initial review with user

4. Face-to-Face Discussions
   Line-by-line access reviews during interviews of all managers

5. Iterative Negotiation Process
   Multiple rounds of negotiations help resolve contested permissions

6. Role Optimization
   Information Security maps permissions to minimize roles

7. Role-Mapping Validation
   Information Security negotiates mapping of roles to users with managers

Example Manager

Manager’s Reports
• Access to 48 systems
• Access controlled using 3,938 individual permissions

Access Rights Result

Manager’s Reports
• Access to 20 systems
• Access controlled using two roles that include 556 total permissions

Source: The Progressive Corporation; IREC research.
Operational Process Execution: Having achieved a satisfactory level of response maturity, exemplar firms are harnessing an emerging set of technology tools to prevent and reduce the probability of future threats based on forensics data while considering the business’s ability to withstand risk.

The Next Frontier of Operational Response

Having improved operational response times, organizations are moving toward a more predictive operational posture aligned with the business’s risk profile

Security Operations Maturity Model

\[ \text{Schematic} \]

Operational Goal

- Improve Response Efficiency
- Improve Response Effectiveness
- Reduce Probability of Occurrence

Key Lever

- Process Improvements: Triaged response and chain-of-command protocols
- Intrusion Prevention Tools: Automation to scale response
- Predictive Threat Modeling: Event correlation modeling mapped to unique business risk thresholds

Source: IREC research.
**Operational Process Execution:** Beginning in 2001, Boeing IT managers started spending an increasing proportion of their time patching systems and responding to viruses and worms to keep them from disrupting business processes and transactions. In response, Boeing developed a standardized method of prioritizing patch deployments, which includes a tool to segment response based on organization-specific risk. When an IT vendor announces a vulnerability affecting an operating system, application, or other infrastructure component employed by Boeing, company security analysts initiate a rapid assessment of the company’s specific risk level.

**Enterprise-Wide Patch Deployment Prioritization**

*Business-focused patch prioritization tool allows Boeing to quickly evaluate and communicate the organization’s specific risks of new vulnerabilities*

**Security Monitoring Alert and Response Team (SMART) Web Site**

**Illustrative Project**

**SMART Risk-Assessment Grid**

<table>
<thead>
<tr>
<th>Risk Criteria</th>
<th>Low (1)</th>
<th>Medium (2)</th>
<th>High (4)</th>
<th>Critical (8)</th>
<th>Emergency (16)</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level of Exposure</strong></td>
<td>Low or no usage within the company</td>
<td>Used on a small to moderate number of systems</td>
<td>Installed on most systems but not enabled by default</td>
<td>Installed on most systems and enabled by default</td>
<td>N/A</td>
<td>4</td>
</tr>
<tr>
<td><strong>Business Impact Potential</strong></td>
<td>Little or no business impact</td>
<td>Could cause minor problems if compromised (e.g., prevents IM from working, Web site down)</td>
<td>Could cause moderate problems if compromised (e.g., impacts support tasks)</td>
<td>Could cause major problems if compromised (e.g., stops production, erases data)</td>
<td>N/A</td>
<td>2</td>
</tr>
<tr>
<td><strong>Level of Access Potential</strong></td>
<td>Local, nonprivileged, no access escalation</td>
<td>Nonprivileged access (non-root)</td>
<td>Remote access (with no local account)</td>
<td>Transient access to other system</td>
<td>N/A</td>
<td>2</td>
</tr>
<tr>
<td><strong>Propagation State</strong></td>
<td>No exploit code exists</td>
<td>Proof of concept developed, but not publicly available</td>
<td>Proof of concept publicly available</td>
<td>Propagating within the company and not containable</td>
<td>Propagating within the company and not containable</td>
<td>1</td>
</tr>
</tbody>
</table>

**SMART Vulnerability Tracking**

<table>
<thead>
<tr>
<th>Bulletin #</th>
<th>Release Date</th>
<th>Rating</th>
<th>Boeing Risk</th>
<th>Products Affected</th>
<th>Environment</th>
<th>Mitigation Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS–030</td>
<td>4/13/04</td>
<td>High</td>
<td>Critical</td>
<td>Outlook Express</td>
<td>Servers/Desktop</td>
<td>Patching Complete</td>
</tr>
<tr>
<td>CS–012</td>
<td>5/11/04</td>
<td>High</td>
<td>Medium</td>
<td>Routers</td>
<td>Servers</td>
<td>Patching (83%)</td>
</tr>
<tr>
<td>LX–003</td>
<td>7/11/04</td>
<td>Medium</td>
<td>Medium</td>
<td>Apache</td>
<td>Servers</td>
<td>Testing Patch (50%)</td>
</tr>
</tbody>
</table>

Source: The Boeing Company; IREC research.
Regulatory Compliance Enablement: Year One Sarbanes-Oxley “Postmortems” across the membership found that companies spent a significant amount of resources on Section 404 compliance, as a lack of transparency around requirements and a reliance on external consultants drove up costs. Because of impending deadlines and scarce internal resources, companies’ compliance strategies were often ad hoc, uncoordinated, and placed little emphasis on building ongoing, repeatable processes. As a result, many information risk executives are far from convinced that subsequent compliance efforts will be substantially cheaper than SOX Year One.

### AVOIDING PERPETUAL COMPLIANCE COSTS

**Despite significant investments in SOX-related compliance...**

<table>
<thead>
<tr>
<th>Sarbanes-Oxley Section 404 Implementation Costs</th>
<th>By Company Revenue Bracket</th>
</tr>
</thead>
<tbody>
<tr>
<td>$14,730,000</td>
<td>&gt; $25 Billion</td>
</tr>
<tr>
<td>$9,010,000</td>
<td>$5 Billion–$25 Billion</td>
</tr>
<tr>
<td>$4,320,000</td>
<td>$1 Billion–$4.9 Billion</td>
</tr>
<tr>
<td>$1,070,000</td>
<td>$0.5 Billion–$.99 Billion</td>
</tr>
</tbody>
</table>

*...most companies have yet to automate critical activities...*

Prevalence of Internal Controls Automation

At Companies with Revenues of More Than $1 Billion

- 60% Have No Automated Testing of Controls in Place
- 40% Have Some Type of Automated Testing of Controls in Place

*...threatening to create a permanent cost overhead*

**An Uncertain Future**

“SOX Year One was rushed, uncoordinated, and probably too expensive. At the time, we simply wanted to comply, and we didn’t have an eye toward long-term sustainability. I’m not entirely confident that future iterations will be much easier or cheaper because as of now the processes just are not in place.”

Chief Information Security Officer
Fortune 250 Pharmaceutical

Source: IREC research.
Regulatory Compliance Enablement: In 2002, citing unresolved audit issues, uncoordinated compliance management efforts, and a lack of integration between internal and external auditing reporting processes, Allstate’s Chief Privacy Officer commissioned the creation of a three-FTE Compliance and Policy organization. This group leverages a seven-step compliance management process to identify required controls, assess business unit compliance risk, and drive collaborative mitigation and reporting.

A Process for Continuous Compliance Management

Cross-functional prioritization and communication help to drive collaborative compliance tracking between technology and business areas

Allstate’s Compliance Management Process

1. Priority Setting
   Compliance and Policy group, upon interfacing with IPPGO and corporate stakeholders such as the Chief Privacy Officer, identifies emerging compliance requirements

2. Requirement Mapping
   Customized repository of regulatory requirements allows for standards-setting and continual mapping of required controls

3. Self-Assessment
   Automated tool allows users to create customized assessments based on compliance requirements and provides corresponding remediation plans

4. Project Management
   Based on identified gaps and remediation needs, technology areas collaborate to mitigate risk

5. Compliance Auditing
   Compliance and Policy group assesses technology and business area compliance with respect to corporate policy and standards

6. Compliance Remediation
   Compliance and Policy group works closely with impacted areas to remediate compliance deficiencies

7. Compliance Metrics
   Compliance Desktop tool integrated with Internal Audit’s issue database allows users and management to view or create reports tracking compliance efforts across the enterprise

Source: The Allstate Corporation; IREC research.
End-User Awareness and Education: Understanding that the greatest threats to the enterprise can often come from within, exemplar firms are taking a more targeted, business-attuned approach toward information security awareness. For example, companies are leveraging information risk assessments to ensure that awareness efforts focus on areas and constituencies that can have the greatest impact on the enterprise. Similarly, recognizing that diverse users have varying levels of technical acumen and can perceive messages in different ways, exemplars are tailoring specific awareness campaigns to the unique technology profile of the user.

**Toward Targeted Awareness**

*Exemplar CISOs increase the ROI of awareness campaigns by targeting the most impactful behaviors and tailoring campaign tactics to specific user constituencies*

<table>
<thead>
<tr>
<th>Awareness Investments Focused on Small Set of High-Risk Behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
</tr>
<tr>
<td>Effort</td>
</tr>
</tbody>
</table>

1. Following the 80–20 Rule

2. Tailoring Tactics to Segments

“One Size Fits All” Awareness Campaign

Tactics Tailored to User Constituencies

Source: IREC research.
End-User Awareness and Education: An HSBC review of awareness-raising tactics used by 40 global security groups revealed a plethora of different tactics with little effort to avoid duplicative effort and uneven success across diverse constituencies. As a result, HSBC created an awareness segmentation tool, triaging users by function and linking them with specific tools and campaign plans. Plans are developed locally, with the central Information Security providing consulting services across a 6- to 12-month cycle.

**Targeted Marketing for Information Security**

*Marketing disciplines leveraged to customize security awareness messages for each user segment*

HSBC’s Security Awareness Segmentation Tool

<table>
<thead>
<tr>
<th>Constituency</th>
<th>Training Formats</th>
<th>Marketing Campaigns</th>
<th>Information Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In-Class Training</td>
<td>Gifts</td>
<td>Games</td>
</tr>
<tr>
<td></td>
<td>One-on-One Tutorials</td>
<td>Posters and Flyers</td>
<td>Online Reference Library</td>
</tr>
<tr>
<td></td>
<td>Lunch Briefings</td>
<td></td>
<td>E-Mail Reminders and Alerts</td>
</tr>
<tr>
<td></td>
<td>Online Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training Videos</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Executive Management**: ✓
- **Line Management**: ✓ ✓
- **Sales Reps/Remote Users**: ✓ ✓ ✓
- **IT Developers**: ✓ ✓ ✓
- **IT Operations**: ✓
- **HR Staff**: ✓ ✓ ✓ ✓
- **Finance Staff**: ✓
- **Call Center Staff**: ✓ ✓ ✓ ✓ ✓
- **Branch Staff**: ✓ ✓ ✓ ✓ ✓

Source: HSBC Holdings Plc; CIO Executive Board research.
Performance Measurement and Communication: In their efforts to create reporting processes that truly resonate with diverse audiences, members cite a litany of obstacles, including a dearth of reliable key performance indicators, lack of consensus around what should be measured, and the perennial challenge of quantifying risk.

**Design Guidelines for Building an Exemplar Information Risk Scorecard**

**Each Metric Should…**

- **Enable Decision Making:** Metrics should translate technical security data into business risk implications that executives can leverage to drive mitigation trade-off decisions.
- **Articulate Future Readiness:** Metrics should not only provide a view of current performance but also provide directional guidance on readiness to meet future threat scenarios.
- **Be Comparable Over Time:** Each metric should capture historical trends to outline performance.
- **Require Minimal Resource Consumption:** The data for each metric should be easily and cost-effectively captured.

**The Overall Scorecard Should…**

- **Be Simple:** Performance measurement reports should be concise and quickly highlight areas of concern.
- **Present Nontechnical Data:** The scorecard should speak to an executive audience and focus on nontechnical data.

Source: IREC research.
Performance Measurement and Communication: By querying members across the executive suite, IREC uncovered 20 key areas of concern to include in an Information Risk Scorecard for an executive audience. By creating a high-level composite metric for each question, members can reduce complexity and increase relevance.

### Top Twenty Metrics for the Information Risk Scorecard

*Twenty key questions and corresponding metrics can effectively capture the information risk profile of the enterprise*

#### Holistic Information Risk Scorecard

<table>
<thead>
<tr>
<th>Key Question</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Protection</strong></td>
<td></td>
</tr>
<tr>
<td>1. Are we appropriately prepared for disasters?</td>
<td>Disaster Recovery Readiness</td>
</tr>
<tr>
<td>2. Do IT staff members understand and follow appropriate information security practices?</td>
<td>IT Staff Security Awareness</td>
</tr>
<tr>
<td>3. What technical vulnerabilities jeopardize infrastructure availability and data protection?</td>
<td>Threat Mitigation Effectiveness</td>
</tr>
<tr>
<td>4. How many control lapses are outstanding and what are we doing to remediate them?</td>
<td>Control Lapse Remediation Effectiveness</td>
</tr>
<tr>
<td>5. Are there specific business units that require additional attention in the short-term?</td>
<td>Business Unit Risk Levels</td>
</tr>
<tr>
<td>6. How effective is the information security function at project planning and execution?</td>
<td>Information Security Planning and Project Execution Effectiveness</td>
</tr>
<tr>
<td>7. Does the function have the necessary skills required to meet emerging risk mandates?</td>
<td>Information Security Staff Readiness</td>
</tr>
<tr>
<td>8. How are our information security vendors performing?</td>
<td>Information Security Vendors Effectiveness</td>
</tr>
<tr>
<td><strong>Effectiveness of Compliance and Controls</strong></td>
<td></td>
</tr>
<tr>
<td>9. How can we be sure users that have access to systems have a legitimate business need?</td>
<td>Information Access Control Effectiveness</td>
</tr>
<tr>
<td>10. How protected are we against information risks posed by third-parties?</td>
<td>Third-Party Risk Protection</td>
</tr>
<tr>
<td>11. How effectively have we protected against damage from information security incidents?</td>
<td>Information Security Incident Protection</td>
</tr>
<tr>
<td>12. How effectively does the company respond to incidents?</td>
<td>Incident Response Effectiveness</td>
</tr>
<tr>
<td>13. How compliant are we with IT areas of relevant regulations?</td>
<td>Regulatory Compliance Readiness</td>
</tr>
<tr>
<td><strong>Business Risk Profile</strong></td>
<td></td>
</tr>
<tr>
<td>14. How do information risks threaten our brand and/or long-term reputation?</td>
<td>Brand Risk Protection</td>
</tr>
<tr>
<td>15. How effective are the IT controls of financials systems?</td>
<td>IT Controls of Financial Systems</td>
</tr>
<tr>
<td>16. Is there sufficient separation of duties between roles (for regulatory compliance)?</td>
<td>Separation of Roles Effectiveness</td>
</tr>
<tr>
<td>17. Are information security decisions based on principled risk assessments?</td>
<td>Risk Assessment Adoption</td>
</tr>
<tr>
<td><strong>Internal Performance</strong></td>
<td></td>
</tr>
<tr>
<td>18. Do we pose an information risk to our customers, partners, and other third-parties?</td>
<td>External Information Security Acceptance</td>
</tr>
<tr>
<td>19. What organizational obstacles exist to appropriately mitigating information risks?</td>
<td>Degree of Business Collaboration</td>
</tr>
<tr>
<td>20. Do users understand and follow information security policies?</td>
<td>Awareness Effectiveness</td>
</tr>
</tbody>
</table>

Source: IREC research.
Performance Measurement and Communication: In an effort to reduce the highly technical focus of the first iteration of its scorecard, Barclays’ revised version linked key business priorities to four key categories—Data Security, Technology Security, Online Channels Security, and Governance and Assurance. The scorecard provides high-level trending analysis, CISO-articulated summaries, and supplemental data for corresponding categories.

**Showing Status While Signaling Supporting Data**

*Scorecard identifies priority risks and highlights availability of supporting information without requiring detailed review*

### Information Risk Scorecard

<table>
<thead>
<tr>
<th>Control Area</th>
<th>Indicators</th>
<th>Risk</th>
<th>Trend</th>
<th>Summary</th>
<th>Source: Barclays PLC; IREC research.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Security Objectives</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Confidentiality</td>
<td>Logical Access</td>
<td>○</td>
<td>↑</td>
<td>The risks associated with access to data are being driven down rapidly, as Sarbanes-Oxley and other programs complete their work.</td>
<td></td>
</tr>
<tr>
<td>• Integrity</td>
<td>Cryptography</td>
<td>○</td>
<td>↑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Technology Security Objectives</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Integrity</td>
<td>Firewalls</td>
<td>○</td>
<td>↑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability</td>
<td>Servers</td>
<td>○</td>
<td>↑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability</td>
<td>Desktops</td>
<td>○</td>
<td>↑</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Online Channels Security Objectives</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Authentication</td>
<td>Fraud</td>
<td>○</td>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Privacy</td>
<td>Web Site</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability</td>
<td>Security</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability</td>
<td>Resilience</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Governance and Assurance</strong></td>
<td>Maturity</td>
<td>○</td>
<td>↑</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key Insight**

To simultaneously address executive-level risk concerns and counter fears of poorly founded subjective assessments, scorecards must economically surface key findings while signaling the existence of supporting data.
The CIO and Head of IT Infrastructure’s Role in Information Risk’s Evolution

The transformation of the Information Risk function from a firewall manager to a steward of the corporate brand requires significant coordination and alignment with key internal partners both inside and outside IT. CIOs and heads of IT infrastructure are uniquely positioned to facilitate this evolution by working with information risk executives across three key initiatives:

- **Delineate Clear Information Risk Management Roles and Responsibilities**

  With demands such as regulatory compliance and data privacy expanding the traditional purview of information risk, establish clear governance parameters to avoid duplicative or uncoordinated management efforts. For example, Information Risk often “owns” the role of creating security policies; the roles of IT and Legal—while important—are frequently undefined. Ensure significant cross-functional business and risk perspectives to ensure their applicability across the organization.

- **Build Cross-Business Transparency to Align Information Risk Activities**

  While information risk executives clearly understand the importance of aligning activities to specific business needs, this shift will likely be incremental. To help support this development, the IT leadership can leverage their expertise regarding critical business challenges, line managers’ risk profiles, and the ever-changing audit environment to assist the information risk executive in creating business-attuned policies and processes to re-shape internal perceptions and create a culture of security.

- **Support Ongoing Policy Communication and Enforcement**

  The role of the information risk executives is inherently paradoxical: they play a critical role in mitigating strategic and reputational risk to the enterprise, yet they lack the codified enforcement authority over the actual users who are the source of the risk. IT leadership can address this conflict by working with the information risk executive to ensure that security is built into existing processes and is effectively measured—without sacrificing operational efficiency demands. By building on a wealth of accrued knowledge around business-specific risk, security should be a necessary part of doing business rather than a cumbersome obstacle.

Source: IREC research.
Setting Your Organization’s 2006 Priorities

- Identifying Performance Gaps
- Articulating Key Priorities
Key Attributes of a World-Class Information Risk Organization Serves a Twofold Purpose

- Presents a detailed “competency map” of the Information Risk organization, giving members a clear understanding of the critical attributes of leading Information Risk teams.
- Provides a guided diagnostic exercise that enables Information Risk executives to evaluate their organizations’ current approaches against a standard, and to prioritize the areas of focused improvement based on potential impact on company performance.

Key Attributes of a World-Class Information Risk Organization

**A competency diagnostic**

1. **Strategy and Planning**
   - **Importance**
   - **Performance**

   - 5 = Critical
   - 4 = High Priority
   - 3 = Priority
   - 2 = Low Priority
   - 1 = Not Critical

   - 5 = We excel at this
   - 4 = We are good at this
   - 3 = We are average at this
   - 2 = We are poor at this
   - 1 = We are terrible at this

2. **Architecture Design and Implementation**
   - **Improvement Prioritization Matrix**
   - **Effectiveness**
   - **Importance**
   - **Grading Scale**
   - **Objectives**

3. **Performance Management and Value Demonstration**
   - **Improvement Prioritization Matrix**
   - **Effectiveness**
   - **Importance**

4. **Operational Maintenance and Response**
   - **Disaster Recovery and Business Continuity Planning**
   - **Incident Management**
   - **Patch Management**
   - **Policy Compliance Mechanisms**
   - **Performance Reporting**

5. **Intra- and Inter-Enterprise Collaboration**
   - **Information Risk Monitoring**
   - **Performance Incentives**
   - **Skill Development**
   - **Resource Allocation**
   - **Certification and Training**

6. **Business-Focused Reporting**
   - **Information Risk**
   - **Risk Assessment**
   - **Remediation Planning**
   - **Enforcement Management**
   - **Architecture Design**
   - **Application Security**
   - **Access Management**
   - **External Exposure Protection**

---

© 2005 Corporate Executive Board. All Rights Reserved.
Appendix

Overview of the Information Risk Executive Council
Tapping into a Resource of More Than 2,500 Organizations

The reach of the Corporate Executive Board

Principal CEB practice areas

Partial List of IREC Members
A Unique Value Proposition for Serving the Head of the Information Security or Risk Organization

Our place in your universe

Our value proposition

Schematic of IT Research/Advisory Landscape

Have You Been Asking Yourself These Questions?

Driving Functional Excellence
- How do companies organize their information security or risk functions?
- How are companies communicating the value of information security and risk to executives?

Articulating the Vision for Information Assurance
- What techniques are companies using to manage information risks posed by the extended enterprise?
- How are companies integrating regulatory requirements, policy frameworks, and data retention mandates to develop a policy framework for information assurance?
- What kinds of data classification strategies are companies deploying that ensure technological ease-of-use and end-user compliance?

Creating a Security Operations Blueprint
- What key decision rules drive enterprise-wide identity management strategies?
- How are companies leveraging predictive analysis tools to drive disruptive event modeling?

Our unique assets

Unparalleled Network of Peer Executives
Unrivaled Expertise in Best Practices and Data
Unmetered Service Across the Year
Unbiased Advice
From Start to Finish

*Members efficiently leverage Information Risk Executive Council resources across key management initiatives*

**Member’s Utilization and the Council Information Risk Scorecard Builder**

**Scorecard Mandate**

Member tasked with creating a scorecard for the Information Risk function.

**Information Risk Scorecard Builder**

Member uses IREC’s information Risk Scorecard Builder to design audience-specific dashboards.

**Dedicated Author Conference Sessions**

An IREC analyst walks member through scorecard output and provides additional design guidance.

**Collection of Tools**

A member uses IREC’s tools collected from member companies to inform comparative analysis.

**Peer Networking**

A member discusses failure points in lessons learned with other members with similar experiences.

**Virtual Cohort**

Members exchange ideas on scorecard development with peers during an IREC teleconference.

**Best Practice Research**

A member reads research brief examining the technical and management challenges around successful scorecard rollout.

**Member Benefit**

“I only get 10 minutes a year in front of our Board. This year the entire presentation was devoted to our work with the Council. Using the tools and research they provided, we were able to effectively frame our key strategic initiatives and demonstrate how the Information Security drives value for the enterprise as a whole.”

CISO

Financial Services Company
Insight into Leading Practices on Key Challenges

Initiatives in progress across 2006

Developing a Policy Framework for Information Assurance
- Integrating regulatory requirements into the IT security policy framework
- Developing an actionable data retention and archiving program
- Implementing IT security policy compliance processes across a global organization

Managing Information Risks Posed by the Extended Enterprise
- Improving scalability of third-party due diligence
- Ensuring security of outsourced and offshore IT and business processes
- Protecting intellectual property from partners who are also competitors

Pragmatic Data Classification Strategies for Information Protection
- Developing an implementation-friendly data classification schema
- Decision rules for managing unstructured data
- Integrated data classification with rollout of protection strategies such as encryption

Developing an Enterprise-Wide Identity Management Strategy
- Building an integrated deployment road map
- Decision rules for selecting appropriate user and device authentication mechanisms
- Processes for ongoing monitoring of access controls

Creating a Security Monitoring “Command Center”
- Predictive capabilities for modeling disruptive events
- Implementing intrusion detection services
- Tactics for automating policy adherence tracking

Systematically Auditing Key Information Risks Across the Enterprise
- Developing a range of test scenarios to accommodate the changing nature of threats
- Auditing corporate disaster recovery and business continuity processes

To Obtain Copies of Research
IREC members are welcome to unlimited copies without charge. Electronic copies will also be available at the Council’s Web site, www.irec.executiveboard.com. Alternatively, you may e-mail your order to orders@executiveboard.com or contact our Publications Department at +1-202-777-5921.
The study entitled *Key Developments in the Information Risk Function: A Briefing for Chief Information Officers and Heads of IT Infrastructure* is intended for broad dissemination among senior executives and management within your organization. Members are welcome to unlimited copies without charge. Online ordering is available at [www.irec.executiveboard.com](http://www.irec.executiveboard.com). Alternatively, you can call the Publications Department at 202-777-5921, e-mail your order to orders@executiveboard.com or fax in the order form on this page. Additionally, members interested in reviewing any of the Board’s past strategic research are encouraged to request a listing of completed work.

---

**Study Requested**

<table>
<thead>
<tr>
<th>Study Requested</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Developments in the Information Risk Function</td>
<td>You may order an unlimited number of copies without additional charge.</td>
</tr>
<tr>
<td><em>A Briefing for Chief Information Officers and Heads of IT Infrastructure</em></td>
<td></td>
</tr>
</tbody>
</table>

**CATALOG NO.:** IREC145ZES5

---

**Name & Title**

_____________________________________

**Institution**

_____________________________________

**Address**

_____________________________________

_____________________________________

**Telephone**

_____________________________________

**E-Mail**

_____________________________________

---

**COPY AND FAX TO:**

Information Risk Executive Council
+1-202-777-5822

---

*Information Risk Executive Council™*

© 2005 Corporate Executive Board. All Rights Reserved.